On the non-randomness of modular arthmetic progressions : a solution to a problem by V.I. Arnold

Eda Cesaratto, Alain Plagne, Brigitte Vallée

*Discrete Mathematics and Theoretical Computer Science*DMTCS vol. **(subm.)**, by the authors, 1–1

On the non-randomness of modular arithmetic progressions: a solution to a problem by V. I. Arnold

Eda Cesaratto[1] and Alain Plagne[2] and Brigitte Vallée[1]

[1] *GREYC, UMR 6072 du CNRS, Université de Caen, 14032 Caen, France*
[2] *Centre de Mathématiques Laurent Schwartz, UMR 7640 du CNRS, École polytechnique, 91128 Palaiseau Cedex, France*

received March 31, 2006, accepted June 8, 2006.

We solve a problem by V. I. Arnold dealing with "how random" modular arithmetic progressions can be. After making precise how Arnold proposes to measure the randomness of a modular sequence, we show that this measure of randomness takes a simplified form in the case of arithmetic progressions. This simplified expression is then estimated using the methodology of dynamical analysis, which operates with tools coming from dynamical systems theory. In conclusion, this study shows that modular arithmetic progressions are far from behaving like purely random sequences, according to Arnold's definition.

Keywords: modular arithmetic progressions, Arnold's problems, dynamical analysis, transfer operators, Dirichlet series, Perron Formula, bounds à la Dolgopyat

1 Introduction, notations and basic facts

There is a Russian tradition of formulating promising open problems during seminars with a view to promote research. One of the most famous Moscow seminar is led since the 1950's by Vladimir Igorevich Arnold. His complete collection of problems, known as "Zadachi Arnolda", has been recently translated and published in English [2]. One of the most recent problems (Problem 2003-2 of [2]) is concerned with the understanding of what Arnold calls the *randomness of arithmetic progressions*.

1.1 Pseudo-random sequences.

Is it possible to produce, in an *efficient* deterministic way, sequences which resemble *enough* "true" *random* sequences? In pseudo-random number generation, randomness is limited to the choice of the starting point (the "seed"), and, after this starting point, the process is totally deterministic. Such sequences are called pseudo-random. There is a compromise to be found, between the efficiency for producing such sequences, and their quality with respect to randomness.

What is a "random" sequence? From J.N. Franklin (1962) cited in the book of Knuth [9]: "A sequence is random if it has every property that is shared by all infinite sequences of independent samples of random variables from the uniform distribution", and, from Lehmer (1951): "In such a sequence, each term is unpredictable to the uninitiated, and the digits pass a certain number of tests, traditional with statisticians...." The book of Knuth [9] is a central contribution to the subject. There, Knuth tries to make these statements more precise and he defines precisely a family of "good" statistical tests. In this context, a statistical test is an efficient algorithm which is able to distinguish (in a significant way) "random" sequences from other sequences. With the help of a threshold, it answers "yes" if the sequence resembles enough a random sequence (according to this precise test), and "no" if this is not the case.

The Linear Congruential Generator (LCG) is by far the most popular random number generator. With four numbers, the modulus n, the increment a, the multiplier b, and the starting value x_1, the desired sequence of "random" numbers is obtained by setting

$$x_{i+1} = b \cdot x_i + a \pmod{n} \qquad \text{for } i \geq 2 \quad \text{and} \quad x_1 = 1.$$

This method is used in all computer systems, due to its time efficiency. However, the quality of the LCG is very poor. For instance, it is quite easily predictable [13], even when all the informations are hidden about the quadruple (n, a, b, x_0) and even if the generator is only formed with the most significant bits of the x_i's.

Of course, the quality is even worse with the particular case of a multiplier b equal to 1. In this case, this is just an arithmetic progression, and, if x_1 is chosen to be zero, one obtains a modular arithmetic progression of the form $x_i = (i-1)a \pmod{n}$. Though this is the worst–case of an already very bad scheme, Arnold was interested in studying this random number generator, and he proposed a precise measure for characterising the (bad) quality of such sequences.

1.2 Randomness of modular sequences in Arnold's sense.

Arnold in [3] defines a general characteristic of randomness of a modular sequence. He chooses a normalized mean-value of the square of the distance between consecutive elements in the geometric sense.

Let us introduce this notion more precisely. Given an integer n and a sequence $\underline{x} = (x_i)_{1 \leq i \leq T}$ of T elements of the finite circle $\mathbb{Z}/n\mathbb{Z}$, and denoting by π the canonical projection of $\mathbb{Z}/n\mathbb{Z}$ onto the set of integers $\{0, 1, 2, \ldots, n-1\}$, we set $y_i = \pi(x_i)$. The geometric ordering on the finite circle $\mathbb{Z}/n\mathbb{Z}$ is defined by the permutation σ of $\{1, 2, \ldots, T\}$ for which

$$0 \leq y_{\sigma(1)} \leq y_{\sigma(2)} \leq \cdots \leq y_{\sigma(T)} \leq n-1.$$

The geometric successor of $y_{\sigma(i)}$ (for $i < T$) is $y_{\sigma(i+1)}$ and the geometric successor of $y_{\sigma(T)}$ is $y_{\sigma(1)}$. Finally, the distance between two geometrically consecutive points on the finite circle is defined as

$$\delta_i = \begin{cases} y_{\sigma(i+1)} - y_{\sigma(i)}, & \text{if } 1 \leq i \leq T-1, \\ n + y_{\sigma(1)} - y_{\sigma(T)}, & \text{if } i = T. \end{cases}$$

All the δ_i's are by definition positive and satisfy $\delta_1 + \delta_2 + \cdots + \delta_T = n$. Arnold considers the

normalized mean-value of the square of the δ_i's

$$s = s(n, \underline{x}, T) = \frac{T}{n^2} \sum_{i=1}^{T} \delta_i^2,$$

and he proposes s as a characteristic of randomness of the modular sequence.

The minimum possible value of s is $s = 1$: it is reached when the sequence gives rise to a regular T-gon, since, in this case,

$$s = \frac{T}{n^2} T \left(\frac{n}{T}\right)^2 = 1.$$

More generally, the value of s is close to 1 when the geometric distances between consecutive elements are close to each other.

The maximum value of s is $s = T$: it is obtained in the degenerate case when the sequence $\underline{x}$ assumes only one value, since, in this case

$$s = \frac{T}{n^2} \cdot n^2 = T.$$

More generally, the value of s is close to T when all the geometric distances between consecutive elements are small except one which is then close to n.

On the other hand, a random choice of T independent uniformly distributed points on the finite circle leads to what Arnold calls the "freedom-liking" value $s_*(T)$. Defining two integrals whose domain is the portion $\mathcal{P}$ of the hyperplane of $\mathbb{R}^T$ defined by $x_1 \geq 0, x_2 \geq 0, \dots x_T \geq 0$, $x_1 + \cdots + x_T = 1$,

$$I_1 := \int_{\mathcal{P}} (x_1^2 + \cdots + x_T^2)\, \mathrm{d}x_1 \dots \mathrm{d}x_T = T \cdot \sqrt{T} \cdot \frac{2}{(T+1)!}, \qquad I_2 := \int_{\mathcal{P}} \mathrm{d}x_1 \dots \mathrm{d}x_T = \sqrt{T} \frac{1}{(T-1)!},$$

$$\text{one obtains} \quad s_*(T) = T \cdot \frac{I_1}{I_2} = \frac{2T}{T+1}, \qquad s_*(T) \to 2 \quad \text{for } T \to \infty.$$

From these observations, it can be inferred that, for a given modular sequence, the value of s allows us to evaluate some kind of degree of randomness: if s is "much smaller" than s_*, this means "mutual repulsion", while if s is "much larger" than s_*, this means "mutual attraction". On the opposite side, from these two extremal types of non-randomness, the fact that s is "close" to s_* can be considered as a sign of randomness.

This paper will mainly deal with the case where only two distances Δ and δ appear, with a respective number of occurrences equal to ζ and ξ, so that $n = \zeta\Delta + \xi\delta$. In this case, we may compute

$$s = \frac{\zeta + \xi}{n^2} \cdot (\zeta\Delta^2 + \xi\delta^2) = 1 + \zeta \cdot \xi \cdot \frac{(\Delta - \delta)^2}{(\zeta\Delta + \xi\delta)^2}. \tag{1}$$

1.3 Arnold's problem: the case of arithmetic progressions

Having defined a criterion of randomness for modular sequences, we may focus on a particular type of sequences, and ask if this type of sequence has a random behaviour or not. Arnold's problem 2003-2 aims at studying the randomness of modular arithmetic progressions: let a and

n be two coprime integers and fix another integer T satisfying $0 < T < n$. With the constraints on a, n and T, the sequence $\underline{x} = (x_i)_{1\leq i\leq T} \in (\mathbb{Z}/n\mathbb{Z})^T$ given by

$$x_i \equiv (i-1)a \pmod{n}, \qquad \text{for } 1 \leq i \leq T,$$

is formed with distinct elements[(i)]. Remind that such an arithmetic modular progression is a particular case of a linear congruential generator $x_{i+1} = bx_i + a \pmod{n}$ with $x_1 = 0$ and $b = 1$.

The main question is the following: For a random triple (a, n, T), with a and n coprime, and $T < n$, what is the expected value of $s(n, a, T) = s(n, \underline{x}, T)$? Arnold proposes two ways of choosing randomly the parameter T, when n is large and a is coprime and random modulo n:

(*i*) T is random in $1 \leq T \leq n/2$,

(*ii*) T is one of the denominators of the k-th continued fraction approximation (usually called k-th convergent) of the number a/n, that is writing

$$\frac{a}{n} = \cfrac{1}{m_1 + \cfrac{1}{m_2 + \cfrac{1}{\ddots + \cfrac{1}{m_p}}}} = [m_1, m_2, \ldots, m_p],$$

we choose $T = q_k$ to be the denominator of the fraction $[m_1, m_2, \ldots, m_k] = \dfrac{p_k}{q_k}$.

We will be mainly interested in the second type of choice. Arnold proposes to study and hopefully understand (mainly from an experimental viewpoint) the behaviour of $s(n, a, T) = s$ when $T = q_k$ is one of the denominators of the truncated continued fraction of a/n. In particular, when the choice of the index k will be made precise as a function of the pair (a, n), one may ask what is the asymptotic behaviour of the average of $s(n, a, q_k)$ on the set

$$\omega_n := \{(a, n); \quad 1 \leq a \leq n, \gcd(a, n) = 1\}. \tag{2}$$

In this paper, we concentrate mainly on this situation and shall prove a quite precise result for which we need some definitions first.

1.4 Main result.

Here, we consider the set $\Omega = \{(u, v) \in \mathbb{N}^2; \quad 1 \leq u < v, \ \gcd(u, v) = 1\}$ which is the union of all the ω_n's defined in (2). For a pair $(u, v) \in \Omega$, $P(u, v)$ is the depth of the (proper) continued fraction expansion of u/v. We are interested in the behaviour of the Arnold sum $s(v, u, q_k)$ when the index k itself depends on the pair (u, v) *only via* the depth $P(u, v)$. More precisely, we consider the case when k is related to some fixed function $F : \mathbb{N} \to \mathbb{N}$ (with $1 \leq F(p) \leq p$) via the equality $k = F(P(u, v))$, and we deal with particular functions F which will be said to be *admissible*.

(i) In fact, we have translated everything by a $-a$ compared to what Arnold defines.

Definition 1 *A function $F : \mathbb{N} \to \mathbb{N}$ is said to be admissible if there exist two real numbers $a > 0$ and $b < 1$ such that for any integer p, one has $a\,p \leq F(p) \leq b\,p$.*

In the sequel, for any admissible function F, we consider the random variable, denoted by $S_{<F>}(u, v)$ and defined as

$$S_{<F>}(u, v) := s(v, u, q_k) \qquad \text{with} \quad k := F(P(u, v)) \tag{3}$$

in Arnold's notation. For any integer $N > 0$, the subset Ω_N of Ω formed of pairs (u, v) whose denominator v is at most equal to N,

$$\Omega_N = \{(u, v) \in \Omega; \quad v \leq N\} = \{(u, v) \in \mathbb{N}^2; \quad 1 \leq u < v,\ \gcd(u, v) = 1, \quad v \leq N\} \tag{4}$$

is equipped with the uniform probability. Remark that this is the union of sets ω_n defined in (2) for $n \leq N$. We wish to study the asymptotic behaviour of the mean value of $S_{<F>}$ on Ω_N. Here is our main result:

Theorem 1 *Let F be any admissible function and $S_{<F>}$ be the random variable defined in* (3)*. The mean value of $S_{<F>}$ on the set Ω_N satisfies*

$$\mathbb{E}_N[S_{<F>}] = A + O(N^{-\alpha}), \qquad \textit{with} \quad A = \frac{2}{3} + \frac{1}{4 \log 2} = 1.027\ldots$$

The constant A does not depend on F, whereas the exponent $\alpha > 0$ depends on F.

This theorem first implies that modular arithmetic progressions are not random at all (from Arnold's point of view). This is by no mean a surprise since it is difficult to imagine a sequence which would be more predictable than an arithmetic progression: nobody would have ever thought to use it as a device to produce random numbers! However, our theorem provides a precise estimate for quantifying this non-randomness, and asserts that this estimate does not depend on the choice of the admissible function F. This estimate would have been difficult to conjecture with elementary means. Even starting from the results of Section 2 (which already show a high regularity in the pattern of the δ_i's which enter the definition of s), it is not clear how to derive any useful bound on s.

Our result can also be interpreted as another precise fact in the zoology of the basic theory of arithmetic progressions. It can viewed as a metric version of the classical two distance theorem [see Section 2.2].

1.5 Plan of the paper.

Section 2 provides a first reduction of the Arnold problem, and expresses the Arnold sum as a function of the so–called continuants, relative to continued fraction expansions. These quantities are then estimated in Section 3, with various tools: Dirichlet series, Perron's formula, transfer operators, bounds à la Dolgopyat.

2 A first reduction of the Arnold problem: using the Three Distance Theorem and continuants.

This section is devoted to obtain a precise expression of $S_{<F>}(u,v)$ as a function of the so-called continuants of the continued fraction of u/v. This is made possible by using the three-distance theorem. For this section, the interested reader may consult [1].

2.1 Continued fractions

We recall the basics of continued fractions and Euclidean algorithm. On the input (u,v) (with $0<u<v$), the Euclidean algorithm builds the sequence of remainders (v_i). With $v_0 := v, v_1 := u$, it computes a sequence of Euclidean divisions

$$v_0 = m_1 v_1 + v_2, \quad v_1 = m_2 v_2 + v_3, \quad \dots \quad v_{p-2} = m_{p-1} v_{p-1} + v_p, \quad v_{p-1} = m_p v_p + 0. \tag{5}$$

The quotients m_i satisfy $m_i := \lfloor v_{i-1}/v_i \rfloor$ and the algorithm stops when $v_{p+1} = 0$. This process decomposes the rational number u/v as a finite continued fraction

$$\frac{u}{v} = \cfrac{1}{m_1 + \cfrac{1}{m_2 + \cfrac{1}{\ddots + \cfrac{1}{m_p}}}} = [m_1, m_2, \dots, m_p]. \tag{6}$$

The integer p is called the *depth* of the continued fraction. A truncation of the continued fraction expansion at depth k produces two rationals:

(i) the *beginning rational*, which is often called the *k-th convergent* of u/v,

$$\frac{p_k}{q_k} := [m_1, m_2, \dots, m_k], \tag{7}$$

(ii) the *ending rational*, which is the ratio of two successive remainders,

$$\frac{v_{k+1}}{v_k} = [m_{k+1}, m_{k+2}, \dots, m_p]. \tag{8}$$

If we let $p_0 = 0,\ q_0 = 1$, it is well known that the sequences of numerators and denominators verify respectively $p_1 = 1, q_1 = m_1$ and the recursion formula, for $2 \le i \le p$,

$$p_i = m_i p_{i-1} + p_{i-2}, \qquad q_i = m_i q_{i-1} + q_{i-2}.$$

Then, for any positive integer i with $1 \le i \le p-1$, the following equalities hold,

$$q_i v_i + q_{i-1} v_{i+1} = v_0 \qquad q_i v_1 - p_i v_0 = (-1)^i v_{i+1}, \tag{9}$$

(as can be seen by an immediate induction argument) and will be used later. Here, we mainly use the denominators q_k, v_k of these sequences, also called the continuants: q_k is the beginning continuant of order k, and v_k is the ending continuant of order k.

2.2 The three-distance theorem

We shall make a central use of the three-distance theorem conjectured by Steinhaus and proved by Surányi [14], Sós [12] and Świerczkowski [15].

The three-distance theorem is concerned with arithmetic progressions modulo 1, an object very close to modular arithmetic progressions. A *circular sequence with difference* α is thus defined as a finite arithmetic progression on the torus $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ without repetition, that is a sequence $(x_i)_{0\leq i\leq T-1} \in \mathbb{T}^T$ such that $x_i \neq x_j$ for $i \neq j$ and $x_{i+1} - x_i = \alpha$ is independent of i when $0 \leq i \leq T-2$. We have a notion of geometric successor on the torus exactly in the same way as in the case of modular arithmetic progressions on the finite circle. We define the *successor function* j as the bijection of $\{0, 1, \ldots, T-1\}$ which associates to an index i the one of the geometric successor of x_i. To a circular sequence, we associate its two *parameters*: these are the two integers ζ and ξ of $\{0, 1, \ldots, T-1\}$ satisfying $j(\zeta) = 0$ and $j(0) = \xi$. It can be easily seen (see Proposition 1.3 in [6]) that $T \leq \zeta + \xi$.

The three-distance theorem asserts that the function $i \mapsto j(i) - i$ takes at most three values:

Theorem A. [Three-distance theorem.] *Let $(x_i)_{0\leq i\leq T-1} \in \mathbb{T}^T$ be a circular sequence with parameters ζ and ξ, then the function $i \mapsto j(i) - i$ satisfies*

$$j(i) - i = \begin{cases} \xi & \text{if } 0 \leq i \leq T - \xi - 1 \\ \xi - \zeta & \text{if } T - \xi \leq i \leq \zeta - 1 \\ -\zeta & \text{if } \zeta \leq i \leq T - 1. \end{cases}$$

Notice that the first and third intervals defining j are never empty. However, in the equality case $T = \zeta + \xi$, the interval in the middle is empty. The function $i \mapsto j(i) - i$ takes in this case only two values: we call it a *two-distance sequence*. Therefore, j is a two distance sequence if and only if the sum of its two parameters is equal to the cardinality of the sequence.

In the general case, there exist three distances, say $0 < \delta_1 < \delta_2 < \delta_3$, considered as positive real numbers less than 1 [which gives its name to this theorem]. They are respectively equal to $\xi\alpha, (\xi - \zeta)\alpha$ and $-\zeta\alpha$ modulo 1: we observe that $\delta_i + \delta_j \equiv \delta_k \pmod 1$. Since, by definition, we must have $\delta_1 + \delta_2 + \delta_3 \leq 1$, one has $0 < \delta_i + \delta_j < 1$ therefore $\delta_i + \delta_j = \delta_k$ which means that the two smallest distances sum to the largest one.

This theorem is highly related to the theory of Farey approximations. We recall that an irreducible fraction a/b is a Farey approximation of some real number α if there is no other fraction with denominator less than or equal to b in the interval delimited by α and a/b.

The following result (Corollary 2.6 of [6]) is useful:

Theorem B. *If t is the denominator of a Farey approximation of the real number α, then any circular sequence with difference α of t elements is a two-distance sequence.*

2.3 Reducing Arnold's measure of randomness

The next result provides an alternative expression of the Arnold sum as a function of (beginning and ending) continuants:

Proposition 2 *Let (u, v) be an element of Ω, and consider the two sequences of continuants of the rational u/v, (q_k) and (v_k). Consider the arithmetic progression $\underline{x} := (x_i)_{1\leq i\leq q_k} \in (\mathbb{Z}/n\mathbb{Z})^{q_k}$ defined by $x_i \equiv (i-1)u \pmod v$ for $1 \leq i \leq q_k$.*

Then the distance between geometrically consecutive elements of the sequence $\underline{x}$ *on the discrete circle equals either* v_k *or* $v_k + v_{k+1}$*. More precisely, there are exactly* q_{k-1} *such distances equal to* $v_k + v_{k+1}$ *and* $q_k - q_{k-1}$ *equal to* v_k*. In particular, we have*

$$s(v,u,q_k) = \frac{1}{v_0^2}\,\big(\, q_k^2 v_k^2 \,+\, 2q_{k-1}q_k v_k v_{k+1} \,+\, q_{k-1}q_k v_{k+1}^2 \,\big) = 2\frac{q_k v_k}{v_0} - \frac{q_k^2 v_k^2}{v_0^2} + \frac{q_k v_{k+1}}{v_0} - \frac{q_k^2 v_k v_{k+1}}{v_0^2} \tag{10}$$

Proof: By definition, q_k is the denominator of a convergent of u/v. It is therefore in particular the denominator of a Farey approximation of u/v.

Let us now consider the sequence $(u_i)_{0\le i\le q_k-1}$ defined by $u_i = \{x_{i+1}/v\} = \{iu/v\}$ (the notation $\{\}$ means fractional part). It is clearly a circular sequence. By what we have just said and Theorem B, it is a two-distance sequence. Write ζ and ξ for its two parameters.

Going back to the sequence (x_i) itself, this tells us that two lengths of interval appear on the finite circle, δ and Δ, say. One of these distances is given by the best approximation of u/v by rational numbers having a denominator less than $q_k - 1$, namely p_{k-1}/q_{k-1}, which implies that one of the parameters of the sequence is $\zeta = q_{k-1}$ and

$$\delta = |q_{k-1}u - p_{k-1}v| = |q_{k-1}v_1 - p_{k-1}v_0| = v_k,$$

by (9). Since for a two-distance sequence, $\zeta + \xi$ coincide with the cardinality of the sequence, it follows that $\xi = q_k - q_{k-1}$. Since

$$|(q_k - q_{k-1})u - (p_k - p_{k-1})v| = |(q_k v_1 - p_k v_0) - (q_{k-1}v_1 - p_{k-1}v_0)| = |v_{k+1} + v_k| = v_k + v_{k+1},$$

it follows that $\Delta = v_k + v_{k+1}$. To find the number of intervals of each of these two lengths, first observe that these numbers are uniquely determined and then that the Bezout relation (9) tells

$$q_k v_k + q_{k-1}v_{k+1} = v_0 = v.$$

In view of this, we deduce the relation $(q_k - q_{k-1})\delta + q_{k-1}\Delta = v$, which entails that there are exactly q_{k-1} intervals of length $v_k + v_{k+1}$ and $q_k - q_{k-1}$ of length v_k.

Finally, we obtain the expression of $s(v,u,q_k)$ as a function of the two sequences (q_k) and (v_k),

$$s(v,u,q_k) = \frac{q_k}{n^2}\big(q_{k-1}(v_k + v_{k+1})^2 + (q_k - q_{k-1})v_k^2\big) = \frac{1}{v_0^2}\big(q_k^2 v_k^2 + 2q_{k-1}q_k v_k v_{k+1} + q_{k-1}q_k v_{k+1}^2\big).$$

In the sequel, it proves more convenient to deal with expressions which involve beginning continuants q_i's and ending continuants v_j's with indices i and j satisfying $0 \le j - i \le 1$. With (9), each occurrence of $q_{k-1}v_{k+1}$ can be replaced by $v_0 - q_k v_k$, and the second expression of (10) follows. □

3 Dynamical analysis of the Arnold sum.

We wish to evaluate the mean value of the expression (10) obtained in Proposition 2, namely

$$S(u,v) := S_1(u,v) + S_2(u,v) + S_3(u,v) + S_4(u,v)$$

with

$$S_1(u,v) = 2\frac{1}{v_0}\, q_k v_k, \quad S_2(u,v) = -\frac{1}{v_0^2}\, q_k^2 v_k^2, \quad S_3(u,v) = \frac{1}{v_0}\, q_k v_{k+1}, \quad S_4(u,v) = -\frac{1}{v_0^2}\, q_k^2 v_k v_{k+1}. \tag{11}$$

[We recall that we let $u = v_1$, $v = v_0$ and $k = F(P(u,v))$]. We shall consider the following Dirichlet series

$$T_i(s) = \sum_{(u,v)\in\Omega} \frac{S_i(u,v)}{v^{2s}}, \qquad T(s) := \sum_{i=1}^{4} T_i(s) = \sum_{(u,v)\in\Omega} \frac{S(u,v)}{v^{2s}} = \sum_{n\geq 1} \frac{a_n}{n^{2s}}, \tag{12}$$

relative to the parameters S_i, S, together with the Dirichlet series

$$T_0(s) := \sum_{(u,v)\in\Omega} \frac{1}{v^{2s}} = \sum_{n\geq 1} \frac{b_n}{n^{2s}}. \tag{13}$$

Since the coefficients a_n and b_n are respectively equal to

$$a_n := \sum_{(u,n)\in\Omega} S(u,n), \qquad b_n := \sum_{(u,n)\in\Omega} 1.$$

the expectation $\mathbb{E}_N(S_{<F>})$ involves partial sums of a_n, b_n under the form

$$\mathbb{E}_N(S_{<F>}) = \frac{\Phi(N)}{\Phi_0(N)}, \qquad \text{with} \quad \Phi(p) := \sum_{n\leq p} a_n, \quad \Phi_0(p) := \sum_{n\leq p} b_n. \tag{14}$$

We then proceed with three main steps, which define the general method of the dynamical analysis described for instance in [17]:

Step 1. We look for alternative forms of the Dirichlet series $T_i(s)$ which involve the transfer operators of the underlying dynamical system.

Step 2. We then study the "dominant" singularities of $T_i(s)$, in particular the behaviour of $T_i(s)$ when $\Re s$ is near 1.

Step 3. We finally transfer the informations about singularities into asymptotic estimates of the coefficients a_n, b_n, and we obtain the estimate of Theorem 1. Since we wish to obtain estimates with remainder terms, we use the Perron Formula (for a description of this formula, see for instance [16]). The Perron formula (of order two) applied to our series $T(s)$, with a vertical line $\Re s = D > 0$ inside the domain of convergence of T says that

$$\Psi(U) := \sum_{p\leq U} \sum_{n\leq p} a_n = \frac{1}{2i\pi} \int_{D-i\infty}^{D+i\infty} T(s) \frac{U^{2s+1}}{s(2s+1)}\, \mathrm{d}s. \tag{15}$$

For using it with some success, we wish to deform the integration contour and need precise informations about $T(s)$, in particular when s belongs to vertical strips near $s = 1$ [this is the rôle of Step 2]. Then, we shall transfer the estimates on $\Psi(U)$ into estimates on $\Phi(p)$, as in [4] and [5].

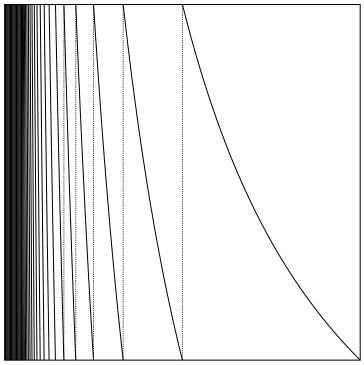

Fig. 1: Euclidean dynamical system

3.1 The Euclidean dynamical system. Transfer operators

We first look for alternative forms of Dirichlet series as means of various transfer operators. We now recall this notion.

When computing the gcd of the integer-pair (u, v), the Euclid algorithm performs a sequence of p divisions [see (5)]. Each division $v = mu + r$ replaces the pair (u, v) by the new pair (r, u). The map U which replaces the rational u/v by the rational r/u is defined by

$$U(x) = \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor, \qquad U(0) = 0,$$

and can be extended to the real interval $\mathcal{I} = [0, 1]$. The pair $(\mathcal{I}, U)$ defines the so–called dynamical system relative to the Euclid algorithm, described in Figure 1. The set of the inverse branches of U is exactly the set

$$\mathcal{H} = \left\{ h(x) = \frac{1}{m + x}; \quad m \in \mathbb{N}, m \geq 1 \right\}.$$

The set $\mathcal{H}^p$, namely $\mathcal{H}^p = \{h = h_1 \circ \cdots \circ h_p; \quad h_i \in \mathcal{H} \ (1 \leq i \leq p)\}$ is the set of inverse branches of U^p. One then associates via (6) to each execution of the algorithm a unique linear fractional transformation (LFT in shorthand notation) h whose depth is exactly the number p of divisions performed. We let $\mathcal{H}^\star := \cup \mathcal{H}^n$.

The main tool of dynamical analysis is the transfer operator introduced by Ruelle (see [11]), denoted by $\mathbf{H}_s$. It generalizes the density transformer $\mathbf{H}$ that describes the evolution of the density: if $f = f_0$ denotes the initial density on $\mathcal{I}$, and f_1 the density on $\mathcal{I}$ after one iteration of S, then f_1 can be written as $f_1 = \mathbf{H}[f_0]$, where $\mathbf{H}$ is defined by

$$\mathbf{H}[f](x) = \sum_{h \in \mathcal{H}} |h'(x)| \cdot f \circ h(x). \tag{16}$$

It is useful to introduce a more general operator that depends on a complex parameter s, with

$\Re s > 1/2$,

$$\mathbf{H}_s[f] = \sum_{h\in\mathcal{H}} |h'|^s \cdot f\circ h. \tag{17}$$

Multiplicative properties of derivatives then entail

$$\mathbf{H}_s^n[f] = \sum_{h\in\mathcal{H}^n} |h'|^s \cdot f\circ h, \qquad (\mathrm{Id} - \mathbf{H}_s)^{-1} := \sum_{n\geq 0} \mathbf{H}_s^n = \sum_{h\in\mathcal{H}^\star} |h'|^s \cdot f\circ h.$$

Since each h is a LFT, the derivative $h'(x)$ can be expressed with the denominator D defined by

$$D[g](x) = cx + d, \text{ for } g(x) = \frac{ax+b}{cx+d} \text{ with } \gcd(a,b,c,d) = 1,$$

$$\text{as} \qquad h'(x) = \frac{ad-bc}{(cx+d)^2} = \frac{\det h}{D[h](x)^2}. \tag{18}$$

Since all the LFT's of $\mathcal{H}^\star$ have a determinant equal to ± 1, this entails an alternative expression for the continuants q_k, v_k of the rationals u/v defined in (7, 8): consider coprime integers u, v for which $u/v = h(0)$, for some $h \in \mathcal{H}^\star$. Then, the total LFT $h = h_1 \circ h_2 \circ \cdots \circ h_p$ decomposes as $h = g \circ \ell$, with

$$g = h_1 \circ h_2 \circ \cdots \circ h_k, \qquad \ell = h_{k+1} \circ h_{k+2} \circ \cdots \circ h_p,$$

so that, with relation (18) and definitions of continuants given in (7,8),

$$\frac{1}{v^2} = \frac{1}{v_0^2} = |h'(0)| = |g'(\ell(0))| \cdot |\ell'(0)|, \qquad \frac{1}{q_k^2} = |g'(0)|, \qquad \frac{1}{v_k^2} = |\ell'(0)|. \tag{19}$$

This explains why the transfer operators will play a fundamental rôle, since they generate the continuants.

3.2 Step 1. Alternative forms for Dirichlet series $T_i(s)$.

Here, the plain operator $\mathbf{H}_s$ is not sufficient for generating expressions of interest. We are led to introduce other transfer operators, that can be viewed as generalisations of the plain operator $\mathbf{H}_s$. The main transfer operators which will be used appear in Figure 2, and the set

$$\mathcal{G}_s := \{\mathbf{H}_s\} \bigcup \mathcal{G}_s^{(0)} \bigcup \mathcal{G}_s^{(1)} \qquad \text{with} \qquad \mathcal{G}_s^{(0)} := \{\mathbf{H}_{(s,\cdot)}\}, \qquad \mathcal{G}_s^{(1)} := \{\mathbf{H}_{(s+t,-t)}; t\in\mathbb{R}\}, \tag{20}$$

plays a central rôle in the sequel. The operators of the set $\mathcal{G}_s^{(1)}$ are used to generate in "parallel" several values of the derivatives, at various points. They have already be introduced in [18], and studied in [18], [5]. The operator $\mathbf{H}_{(s,\cdot)}$ of the set $\mathcal{G}_s^{(0)}$ is mainly used for the generation of beginning continuants, and this is its first occurrence in dynamical analysis.

The main result of this section 3.2 relates Dirichlet series with these various transfer operators.

Proposition 3 *Each Dirichlet series $T_i(s)$ defined in Equations (11,12,13) involves an operator $\mathbf{M}_i(s)$ under the form $T_i(s) = \mathbf{M}_i(s)[\underline{1}](\underline{0})$ where $\mathbf{M}_i(s)$ is an operator acting on the space $\mathcal{C}^1(\mathcal{I}^{q_i})$,*

Number q of variables	Name of the operator	Definition of the component operator when acting on a function $F \in \mathcal{C}^1(\mathcal{I}^q)$
1	$\mathbf{H}_s$	$\lvert h'(x)\rvert^s \cdot F \circ h(x)$
2	$\mathbf{H}_{(s,t)}$	$\lvert h'(x)\rvert^s \cdot \lvert h'(y)\rvert^t \cdot F(h(x), h(y))$
2	$\mathbf{H}_{(s,\cdot)}$	$\lvert h'(x)\rvert^s \cdot F(h(x), y)$

Fig. 2: Definition of operators via their component operators. In each case, the transfer operator is the sum of its component operators, the sum being taken on the set $\mathcal{H}$.

$\underline{1}$ *is the function of q_i variables everywhere equal to 1, and* $\underline{0}$ *is a zero vector of dimension q_i. Moreover, each operator $\mathbf{M}(s) := \mathbf{M}_i(s)$ has the following general form (depending on index i),*

$$\mathbf{M}(s) = \sum_p \mathbb{G}_s^{p-F(p)-1} \circ \mathbf{A}_s \circ \mathbb{L}_s^{F(p)-1},$$

where $\mathbb{G}_s$ and $\mathbb{L}_s$ belong to the set $\mathcal{G}_s$ defined in (20) and $\mathbf{A}_s$ is bounded near $s = 1$.

Proof: We consider three cases, first the series $T_0(s)$, then the series $T_i(s)$ for $i = 1, 2$, finally the two series $T_i(s)$ for $i = 3, 4$.

Case of T_0. Of course, $T_0(s)$ admits a classic alternative expression, of the form $T_0(s) = \zeta(2s-1)/\zeta(2s)$, from which it is easy to perform the three steps of our method. But, it will be useful to also obtain an expression which involves transfer operators. The continued fraction decomposition of u/v is

$$\frac{u}{v} = \frac{v_1}{v_0} = h(0) \qquad \text{with} \quad h := h_1 \circ h_2 \circ \cdots \circ h_p, \qquad \text{and} \quad p = P(u, v).$$

Then, for coprime (u, v),

$$\frac{1}{v^2} = \frac{1}{v_0^2} = |h'(0)| \qquad \text{so that} \quad T_0(s) = \mathbf{M}_0(s)[1](0) \qquad \text{with} \quad \mathbf{M}_0(s) = \sum_p \mathbf{H}_s^p = (I - \mathbf{H}_s)^{-1}. \tag{21}$$

Case of T_1 and T_2. Costs S_1 and S_2 defined in (11) involve the product $q_k v_k$, and the decomposition (19) entails

$$\frac{1}{v^{2s}} S_1(u, v) = 2|g'(\ell(0))|^{s+1/2} |g'(0)|^{-1/2} |\ell'(0)|^s \qquad \frac{1}{v^{2s}} S_2(u, v) = -|g'(\ell(0))|^{s+1} |g'(0)|^{-1} |\ell'(0)|^s.$$

Using the transfer operators $\mathbf{H}_{(s,t)}, \mathbf{H}_{(s,\cdot)}$ defined in Figure 2 provides an alternative form for for $T_i(s)$ $(i = 1, 2)$ as $T_i(s) = \mathbf{M}_i(s)[1](0, 0)$, with

$$\mathbf{M}_1(s) := 2 \sum_{p \geq 1} \mathbf{H}_{(s,\cdot)}^{p-F(p)} \circ \mathbf{H}_{(s+1/2,-1/2)}^{F(p)} \qquad \text{and} \quad \mathbf{M}_2(s) := -\sum_{p \geq 1} \mathbf{H}_{(s,\cdot)}^{p-F(p)} \circ \mathbf{H}_{(s+1,-1)}^{F(p)}. \tag{22}$$

Case of T_3 and T_4. Costs S_3 and S_4 defined in (11) involve products $q_i v_j$ with $j - i = 0$ or 1, and we need a more refined decomposition of the LFT h of the form $h = g \circ a \circ \ell$, with

$$g = h_1 \circ h_2 \circ \cdots \circ h_k, \qquad a := h_{k+1}, \qquad \ell = h_{k+2} \circ h_{k+3} \circ \cdots \circ h_p,$$

which will give rise to a non trivial "middle" operator $\mathbf{A}_s$. With relations

$$\frac{1}{v^2} = \frac{1}{v_0^2} = |h'(0)| = |g'(a \circ \ell(0))| \cdot |a'(\ell(0))| \cdot |\ell'(0)|, \tag{23}$$

$$\frac{1}{q_k^2} = |g'(0)|, \qquad \frac{1}{v_k^2} = |(a \circ \ell)'(0)| = |a'(\ell(0))| \cdot |\ell'(0)|, \qquad \frac{1}{v_{k+1}^2} = |\ell'(0)|,$$

each term $(1/v^{2s})\, S_i(u,v)$, (for $i = 3, 4$) is, with (11, 23), the product of four terms, each of these factors being a product of the same derivative at various points of the interval, namely,

$$|g'(0)|^{-1/2} |g'(a(\ell(0)))|^{1/2+s} |a'(\ell(0))|^{1/2+s} |\ell'(0)|^s, \qquad |g'(0)|^{-1} |g'(a(\ell(0)))|^{s+1} |a'(\ell(0))|^{s+1/2} |\ell'(0)|^s.$$

Using now the transfer operators $\mathbf{H}_{(s,t)}, \mathbf{H}_{(s,\cdot)}$ defined in Figure 2 provides an alternative forms for $T_i(s)$ $(i = 3, 4)$ as $T_i(s) = \mathbf{M}_i(s)[1](0,0)$ with

$$\mathbf{M}_3(s) := \sum_{p \geq 1} \mathbf{H}_{(s,\cdot)}^{p-F(p)-1} \circ \mathbf{H}_{(s+1/2,\cdot)} \circ \mathbf{H}_{(s+1/2,-1/2)}^{F(p)}, \tag{24}$$

$$\mathbf{M}_4(s) := -\sum_{p \geq 1} \mathbf{H}_{(s,\cdot)}^{p-F(p)-1} \circ \mathbf{H}_{(s+1/2,\cdot)} \circ \mathbf{H}_{(s+1,-1)}^{F(p)}. \tag{25}$$

Finally, with (21, 22, 24, 25), Proposition 3 is proven. □

In the following five subsections, we will perform Step 2. We are interested in analytic properties of the operators $\mathbb{G}_s$ of $\mathcal{G}_s$ and we begin in 3.3 by describing the analytic properties of the plain operator $\mathbf{H}_s$. Then, we describe the main spectral properties of generalized operators [Section 3.4] and we focus on the behaviour of these operators when parameter s equals to 1 [Section 3.5]. Finally, we prove in Section 3.6 that the Dirichlet series of interest admit a simple pôle at $s = 1$, and Section 3.7 is devoted to studying these Dirichlet series on vertical strips close to $s = 1$. This will conclude Step 2.

3.3 Step 2. Analytical properties of the plain operator $\mathbf{H}_s$.

We first review some definitions and recall some notions and results about operators and their spectrum. Then, we describe the main spectral properties of the plain operator $\mathbf{H}_s$.

Functional analysis. We consider an operator $\mathbf{L}$ which acts on a Banach space $\mathcal{F}$, endowed with a norm $||.||$.

The *resolvent* $\mathrm{Res}\,(\mathbf{L})$ is formed by the complex numbers λ for which $\mathrm{Id} - \lambda\mathbf{L}$ is invertible. The complement of the resolvent is the *spectrum* $\mathrm{Sp}\,(\mathbf{L})$. An *eigenvalue* is an element λ of $\mathrm{Sp}\,(\mathbf{L})$ for which $\mathrm{Id} - \lambda\mathbf{L}$ is not injective. In this case, the kernel $\mathrm{Ker}\,[\mathrm{Id} - \lambda\mathbf{L}]$ may be finite–dimensional

or not, and there are two sorts of eigenvalues – these of finite multiplicity, or these of infinite multiplicity.

The *spectral radius* $R(\mathbf{L})$ is defined as $R(\mathbf{L}) := \sup\{|\lambda|;\ \ \lambda \in \mathrm{Sp}(\mathbf{L})\}$, and the *essential spectral radius* $R_e(\mathbf{L})$ is the smallest $r \geq 0$ such that any $\lambda \in \mathrm{Sp}(\mathbf{L})$ with modulus $|\lambda| > r$ is an isolated eigenvalue of finite multiplicity. The Spectral Radius Theorem states the equality $R(\mathbf{L}) = \lim_{n\to\infty} ||\mathbf{L}^n||^{1/n}$.

An operator $\mathbf{L}$ is *quasi-compact* if the inequality $R_e(\mathbf{L}) < R(\mathbf{L})$ holds. In this case, the superior part of the spectrum $\mathrm{Sp}(\mathbf{L}) \cap \{|\lambda| > R_e(\mathbf{L})\}$ looks like the spectrum of a compact operator: this is a discrete non empty set formed with spectral elements of type 1. In particular, there is an eigenvalue λ of finite multiplicity for which $|\lambda| = R(\mathbf{L})$. Such an eigenvalue is called a dominant eigenvalue. The *subdominant spectral radius* $R_{sd}(\mathbf{L}) := \sup\{|\lambda|; \lambda \in \mathrm{Sp}\,(\mathbf{L}), |\lambda| \neq R(\mathbf{L})\}$ is strictly less than $R(\mathbf{L})$. The difference $R(\mathbf{L}) - R_{sd}(\mathbf{L})$ defines what is called the *spectral gap*.

A sufficient condition under which an operator can be proven to be quasi–compact is given by the Hennion-Ionescu-Marinescu-Lasota-Yorke theorem.

Theorem C. [Hennion, Ionescu-Tulcea and Marinescu, Lasota-Yorke]. *Suppose that the Banach space $\mathcal{F}$ is endowed with two norms, a weak norm $|.|$ and a strong norm $||.||$, for which the unit ball of $(\mathcal{F}, ||.||)$ is precompact in $(\mathcal{F}, |.|)$. Let $\mathbf{L}$ be a bounded operator on $(\mathcal{F}, ||.||)$. Assume that there exist two sequences $\{r_n\}$ and $\{t_n\}$ of positive numbers such that, for all $n \geq 1$, one has*

$$||\mathbf{L}^n[f]|| \leq r_n \cdot ||f|| + t_n \cdot |f|. \tag{26}$$

Then, the set $\mathrm{Sp}(\mathbf{L}) \cap \{\lambda; |\lambda| > r\}$ with $r := \lim_{n\to\infty} \inf\,(r_n)^{1/n}$ is discrete and formed with eigenvalues of finite multiplicity: the essential spectral radius of the operator $\mathbf{L}$ on $(\mathcal{F}, ||.||)$ satisfies $R_e(\mathbf{L}) \leq r$.

Main Properties of the operator $\mathbf{H}_s$. We first recall the main properties of the plain operator $\mathbf{H}_s$: For $\Re s > 1/2$, it acts on the space $\mathcal{C}^1(\mathcal{I})$ of functions of class $\mathcal{C}^1$ on $\mathcal{I}$. Moreover the contraction ratio, defined as

$$\rho := \lim_{n\to\infty} [\sup\{|h'(x)|; \quad x \in \mathcal{I}, h \in \mathcal{H}^n\}]^{1/n} \tag{27}$$

is strictly less than 1, and an inequality of Lasota-Yorke type holds, for any $\hat{\rho} > \rho$,

$$||\mathbf{H}_s^n[f]||_1 \leq C\,(\hat{\rho}^n \cdot ||\mathbf{H}_\sigma^n||_0 \cdot |||f||_1 + |s| \cdot ||\mathbf{H}_\sigma^n||_0 \cdot ||f||_0)\ , \quad \forall n \geq 1 \tag{28}$$

with $\sigma := \Re s$, $||f||_0 := \sup|f(t)|$, and $||f||_1 := \sup|f(t)| + \sup|f'(t)|$. Then, an easy application of Theorem C, (where the weak norm is the sup-norm $||f||_0$, while the strong norm is the norm $||f||_1$) proves the inequality $R_e(\mathbf{H}_s) \leq \rho R(\mathbf{H}_\sigma)$. Then, the set of spectral values λ of $\mathbf{H}_s$ which satisfy $|\lambda| > \rho R(\mathbf{H}_\sigma)$ is discrete and formed with eigenvalues of finite multiplicity.

When σ is real, the operator $\mathbf{H}_\sigma$ possesses a unique dominant eigenvalue, which is moreover simple. This is due to the mixing properties of the Euclidean dynamical system. By perturbation theory, and thanks to the spectral gap, this remains true when s is a complex number close to 1.

3.4 Step 2, continued. Spectral properties of operators in $\mathcal{G}_s$.

We consider now our generalized operators and we relate their spectrum to the spectrum of the plain operator $\mathbf{H}_s$. We shall prove the following:

Proposition 4 *The following holds for any operator $\mathbb{G}_s \in \mathcal{G}_s$.*

(i) For $\Re s > 1/2$, the operator $\mathbb{G}_s$ acts on the space $\mathcal{C}^1(\mathcal{I}^q)$ of functions of q variables of class $\mathcal{C}^1$ on $\mathcal{I}^q$.

(ii) For s near 1, the operator $\mathbb{G}_s$ has an unique dominant eigenvalue equal to the dominant eigenvalue $\lambda(s)$ of the plain operator $\mathbf{H}_s$, which is separated from the remainder of the spectrum by a spectral gap. The dominant eigenvalue $\lambda(s)$ is simple for $\mathbb{G}_s$ in $\mathcal{G}_s^{(1)}$, whereas it is of infinite multiplicity for $\mathbb{G}_s$ in $\mathcal{G}_s^{(0)}$.

(iii) For any $n \geq 1$, the operator $\mathbb{G}_s^n$ splits as $\mathbb{G}_s^n = \lambda^n(s)\mathbb{P}_s + \mathbb{R}_s^n$, where $\mathbb{P}_s$ is the projector relative to the dominant eigenvalue $\lambda(s)$, the spectral radius of $\mathbb{R}_s$ is strictly less than $\delta|\lambda(s)|$ ($\delta < 1$).

In the proof of this proposition, we shall use differents methods, according as $\mathbb{G}_s$ belongs to $\mathcal{G}_s^{(0)}$ or $\mathcal{G}_s^{(1)}$. We begin by the operators of $\mathcal{G}_s^{(0)}$.

Spectrum of $\mathbb{G}_s$ for $\mathbb{G}_s \in \mathcal{G}_s^{(0)}$. The operator $\mathbf{H}_{(s,\cdot)}$ is closely related to $\mathbf{H}_s$. Denote by F_y the section F_y of F defined as $F_y(x) := F(x,y)$. Then, with the "section" relations

$$\mathbf{H}_{(s,\cdot)}[F](x,y) = \mathbf{H}_s[F_y](x), \qquad (\mathrm{Id} - \lambda\mathbf{H}_{(s,\cdot)})[F](x,y) = (\mathrm{Id} - \lambda\mathbf{H}_s)[F_y](x). \tag{29}$$

it is easy to compare the spectra of $\mathbf{H}_{(s,\cdot)}$ and $\mathbf{H}_s$.

Lemma 5 *For the operator $\mathbb{G}_s = \mathbf{H}_{(s,\cdot)}$ of $\mathcal{G}_s^{(0)}$, the following holds:*
(a) $\mathrm{Sp}\,(\mathbb{G}_s) \subset \mathrm{Sp}\,(\mathbf{H}_s)$.
(b) Any eigenvalue of $\mathbf{H}_s$ is an eigenvalue of $\mathbb{G}_s$, of infinite multiplicity.
(c) For $\Re s = \sigma$, the set $\{\lambda \in \mathrm{Sp}(\mathbb{G}_s); \quad |\lambda| > \rho R(\mathbf{H}_\sigma)\}$ is discrete.
(d) For complex s close enough to 1, the operator $\mathbb{G}_s$ admits a unique dominant eigenvalue (of infinite multiplicity) equal to the dominant eigenvalue $\lambda(s)$ of $\mathbf{H}_s$, separated from the remainder of the spectrum by a spectral gap.

Proof: *(a)* We prove that $\mathrm{Res}(\mathbf{H}_s) \subset \mathrm{Res}(\mathbf{H}_{(s,\cdot)})$. Let λ be an element of $\mathrm{Res}(\mathbf{H}_s)$.
First, we prove that $\mathrm{Id} - \lambda\mathbf{H}_{(s,\cdot)}$ is injective. Suppose that F belongs to the kernel of $\mathrm{Id} - \lambda\mathbf{H}_{(s,\cdot)}$. Then, with (29), any F_y belongs to the kernel of $\mathrm{Id} - \lambda\mathbf{H}_s$. Since $\lambda \in \mathrm{Res}(\mathbf{H}_s)$, this proves that any F_y is zero, and then F itself is zero.
Now, we prove that the range of $\mathrm{Id} - \lambda\mathbf{H}_{(s,\cdot)}$ equals $\mathcal{C}^1(\mathcal{I}^2)$. Consider any function $F \in \mathcal{C}^1(\mathcal{I}^2)$ and prove that F belongs to the range of $\mathrm{Id} - \lambda\mathbf{H}_{(s,\cdot)}$. Since $\lambda \in \mathrm{Res}\,(\mathbf{H}_s)$, any section F_y of F belongs to the range of $\mathrm{Id} - \lambda\mathbf{H}_s$, and, there exists a function $G_y \in \mathcal{C}^1(\mathcal{I})$ such that $F_y = (\mathrm{Id} - \lambda\mathbf{H}_s)[G_y]$. Then, with (29), the function F itself equals $(\mathrm{Id} - \lambda\mathbf{H}_s)[G]$, where G is defined by its sections G_y. The relation $G_y = (\mathrm{Id} - \lambda\mathbf{H}_s)^{-1}[F_y]$ now proves that for any fixed x, the map $y \mapsto G_y(x)$ is of class $\mathcal{C}^1(\mathcal{I})$. Finally, the function G belongs to $\mathcal{C}^1(\mathcal{I}^2)$, and F belongs to the range of $\mathrm{Id} - \lambda\mathbf{H}_{(s,\cdot)}$.

(b) Consider now an eigenvalue λ of $\mathbf{H}_s$, and an eigenfunction ϕ of $\mathbf{H}_s$ relative to λ. With relation (29), any function of the form $\phi(x) \cdot g(y)$ with $g \in \mathcal{C}^1(\mathcal{I})$ is an eigenfunction of $\mathbf{H}_{(s,\cdot)}$ relative to the eigenvalue λ.

(c) This is a consequence of properties of $\mathbf{H}_s$ [see 3.3] and assertion (a).

(d) The relation $R(\mathbb{G}_s) \leq R(\mathbf{H}_s)$ [deduced from (a)], the equality $|\lambda(s)| = R(\mathbf{H}_s)$ [see 3.3], together with assertion (b) prove the first part of (d). Now, the set of the assertion (c) is not empty, and this entails the second part of (d).

□

Spectrum of $\mathbb{G}_s$ for $\mathbb{G}_s \in \mathcal{G}_s^{(1)}$. Any operator of $\mathcal{G}_s^{(1)}$ is also closely related to $\mathbf{H}_s$. All the operators of $\mathcal{G}_s^{(1)}$ coincide "on the diagonal", namely

$$\mathbb{G}_s[F](x,x) = \mathbf{H}_s[\operatorname{diag} F](x), \tag{30}$$

where $\operatorname{diag} F$ is the diagonal of F defined by $\operatorname{diag} F(x) := F(x,x)$. With this diagonal relation (30), it will be easy to compare the spectra of $\mathbb{G}_s$ and $\mathbf{H}_s$.

Lemma 6 *For an operator $\mathbb{G}_s$ of $\mathcal{G}_s^{(1)}$, the following holds:*

(a) For s near 1, $\mathbb{G}_s$ is quasi-compact with essential spectral $R_e(\mathbb{G}_s) \leq \rho R(\mathbb{G}_\sigma)$ with $\sigma := \Re s$.
(b) For real σ, one has $R(\mathbb{G}_\sigma) = R(\mathbf{H}_\sigma)$
(c) If λ is an eigenvalue of $\mathbb{G}_s$ such that $|\lambda| > \rho R(\mathbf{H}_\sigma)$, with $\sigma = \Re s$, then λ is an eigenvalue of the plain operator $\mathbf{H}_s$. Moreover, the multiplicity of λ in $\operatorname{Sp}(\mathbb{G}_s)$ is at most equal to the multiplicity of λ in $\operatorname{Sp}(\mathbf{H}_s)$
(d) For real σ, $\lambda(\sigma) := R(\mathbb{G}_\sigma)$ is an eigenvalue of $\mathbb{G}_\sigma$. For complex s close enough to 1, the operator $\mathbb{G}_s$ admits a unique dominant eigenvalue (simple) equal to the dominant eigenvalue $\lambda(s)$ of $\mathbf{H}_s$, separated from the remainder of the spectrum by a spectral gap.

Proof: A detailed proof can be found in [5].
(a) Operators in $\mathcal{G}_s^{(1)}$ verify a Lasota Yorke bound, that is

$$\|\mathbb{G}_s^n[F]\|_1 \leq C\left(\hat{\rho}^n \cdot \|\mathbb{G}_\sigma^n\|_0 \cdot \|F\|_1 + |s| \cdot \|\mathbb{G}_\sigma^n\|_0 \cdot \|F\|_0\right), \quad \forall n \geq 1 \tag{31}$$

where σ is the real part of s, $\|F\|_0 = \sup|F(x,y)|$ is the sup norm in $\mathcal{C}^0$ and $\|F\|_1 = \|F\|_0 + \|DF\|_0$ is the standard norm of $\mathcal{C}^1$, and $\hat{\rho}$ any number strictly greater than the contraction ratio ρ defined in (27).

(b) The bounded distortion property, namely, the existence of a constant L for which $|h'(x)| \leq L|h'(y)|$ for all x, y in $\mathcal{I}$ and any $h \in \mathcal{H}^\star$, entails, for any $\mathbb{G}_\sigma$, the existence of a constant K, for which the following inequality holds for any $n \geq 1$,

$$\|\mathbb{G}_\sigma^n\|_0 \leq K\|\mathbf{H}_\sigma^n\|_0. \tag{32}$$

On the other hand, the relation $\|\mathbb{G}_\sigma^n[F]\|_0 \geq \|\operatorname{Diag}\mathbb{G}_\sigma^n[F]\|_0 = \|\mathbf{H}_\sigma^n[\operatorname{Diag} F]\|_0$, applied to $F = 1$ entails

$$\|\mathbb{G}_\sigma^n\|_0 \geq \|\mathbb{G}_\sigma^n[1]\|_0 \geq \|\mathbf{H}_\sigma^n[1]\|_0. \tag{33}$$

Equations (32, 33), and the equality $\|\mathbf{H}_\sigma^n[1]\|_0 = \|\mathbf{H}_\sigma^n\|_0$ prove that $\|\mathbf{H}_\sigma^n\|_0 \leq \|\mathbb{G}_\sigma^n\|_0 \leq L\|\mathbf{H}_\sigma^n\|_0$. Now, Relations (28, 31) imply that the spectral radii of $\mathbb{G}_s, \mathbf{H}_s$ in $\mathcal{C}^1$ and $\mathcal{C}^0$ are equal, and, with the Spectral Radius Theorem, this entails the equality

$$R(\mathbf{H}_\sigma) = \limsup_{n\to\infty} \|\mathbf{H}_\sigma^n\|_0^{1/n}, \qquad R(\mathbb{G}_\sigma) = \limsup_{n\to\infty} \|\mathbb{G}_\sigma^n\|_0^{1/n},$$

which proves (b).

(c) With (30), if F is an eigenfunction of $\mathbb{G}_s$ relative to λ, then $\operatorname{diag} F$ is an eigenfunction of $\mathbf{H}_s$ relative to the same λ, *provided that* $\operatorname{diag} F$ *is not identically zero.*

We prove now this fact (by contradiction). To a function F, associate the function $\bar{F}$ defined as $\bar{F}(x,y) = \operatorname{diag} F(x)$. Then the inequality

$$\|\mathbb{G}_s^n[F] - \mathbb{G}_s^n[\bar{F}]\|_0 \leq C \cdot \|F\|_1 \cdot \hat{\rho}^n \cdot \|\mathbf{H}_\sigma^n\|_0 \qquad (\sigma := \Re s), \qquad (\hat{\rho} > \rho) \tag{34}$$

holds. Suppose that F be an eigenfunction of $\mathbb{G}_s$ relative to an eigenvalue λ with $\operatorname{diag} F$ identically zero. Then $\bar{F}$ is also identically zero and this entails with (34)

$$|\lambda^n| \|F\|_0 \leq C \cdot \|F\|_1 \cdot \hat{\rho}^n \cdot \|\mathbf{H}_\sigma^n\|_0. \tag{35}$$

When λ satisfies the inequality $|\lambda| > \rho\, R(\mathbf{H}_\sigma)$, this implies that F is zero on $\mathcal{I}^2$. This is not possible for an eigenfunction. Then, the diagonal function $\operatorname{diag} F$ is not zero. Remark that the same arguments, together with Relation (35), entail that two linearly independent eigenfunctions F_1, F_2 of $\mathbb{G}_s$ give rise to linearly independent diagonal functions $\operatorname{diag} F_1, \operatorname{diag} F_2$. This proves the second part of assertion (b).

(d) Assertions (a) and (b) prove that $\lambda(\sigma) = R(\mathbb{G}_\sigma)$ is an eigenvalue of $\mathbb{G}_\sigma$. With (c), the simplicity of $\lambda(\sigma)$ in $\operatorname{Sp}(\mathbf{H}_\sigma)$ entails the simplicity of $\lambda(\sigma)$ in $\operatorname{Sp}(\mathbb{G}_\sigma)$. Perturbation Theory entails the last assertion. □

Dominant Spectral objects. More generally, with the spectral decomposition given in Proposition 4, with (29) and (30), it is easy to compare the dominant spectral objects of generalized operators in $\mathcal{G}_s$ and the dominant spectral objects of the plain operator $\mathbf{H}_s$.

Proposition 7 *The following holds:*

(i) Operator $\mathbf{H}_{(s,\cdot)}$ of $\mathcal{G}_s^{(0)}$. *The dominant projectors* $\mathbf{P}_{(s,\cdot)}$ *of* $\mathbf{H}_{(s,\cdot)}$ *are related to the dominant spectral objects of* $\mathbf{H}_s$ *[namely, the dominant eigenfunction* ϕ_s*, the dominant projector* $\mathbf{Q}_s$*] via the following equalities*

$$\mathbf{P}_{(s,\cdot)}[F](x,y) = \phi_s(x) \cdot \mathbf{Q}_s[F_y].$$

(ii) Operators of $\mathcal{G}_s^{(1)}$. *The diagonal of the dominant eigenfunction of* $\mathbb{G}_s$ *equals the dominant eigenfunction of the plain operator* $\mathbf{H}_s$*, namely*

$$\operatorname{diag}[\phi_{(s+t,-t)}] = \phi_s.$$

The dominant eigenvector of the dual operator $\mathbb{G}_s^\star$ *applied to some function* F *equals the dominant eigenfunction of the dual operator* $\mathbf{H}_s^\star$ *applied to the diagonal of* F*, namely*

$$\mathbf{Q}_{(s+t,-t)}[F] = \mathbf{Q}_s[\operatorname{diag} F].$$

3.5 Step 2, continued. Explicit dominant eigenfunctions for operators of $\mathcal{G}_s$ at $s = 1$.

We will be interested in the behaviour of the operators $\mathbf{M}_i(s)$ at $s = 1$. From relations (21, 22, 24, 25) the main operators of interest will be $\mathbf{H}_1, \mathbf{H}_{(2,-1)}$ and $\mathbf{H}_{(3/2,-1/2)}$, and we wish to obtain an exact expression of their dominant eigenfunctions. Of course, the dominant spectral objects of $\mathbf{H}_s$ at $s = 1$ are well-known: the dominant eigenfunction ϕ_1 is the Gauss density, defined as

$$\phi_1(x) = \frac{1}{\log 2}\left(\frac{1}{1+x}\right), \qquad \text{and} \quad \mathbf{Q}_1[f] = \int_{\mathcal{I}} f(w)dw. \tag{36}$$

We wish to relate the dominant eigenfunctions $\phi_{(2,-1)}$ and $\phi_{(3/2,-1/2)}$ to ϕ_1.

In the case of two parameters (s, t) with $\Re t > 0, \Re s > 0$, Vallée exhibited in [18] a relation between ϕ_{s+t} and $\phi_{(s,t)}$, namely

$$\phi_{(s,t)}(x, y) = \int_0^1 \beta_{2t,2s}(w)\ \phi_{s+t}(x + (y - x)w)\ \mathrm{d}w$$

where $\beta_{t,s}$ is the classical β density equal to $\beta_{t,s}(w) = \dfrac{\Gamma(s+t)}{\Gamma(s)\Gamma(t)} w^{t-1}(1-w)^{s-1}$.

In the case where $\Re s > 0$ and $t = -1/2$, this equality can be extended as

$$\phi_{(s,t)}(x, y) = \phi_{s+t}(x) + (y - x)\frac{2t}{2s + 2t}\phi'_{s+t}(x),$$

and, in the case where $\Re s > 0$ and $t = -1$, this equality can be extended as

$$\phi_{(s,t)}(x, y) = \phi_{s+t}(x) + (y - x)\frac{2t}{2s + 2t}\phi'_{s+t}(x) + \frac{1}{2}(y - x)^2\frac{2t(2t + 1)}{(2s + 2t)(2s + 2t + 1)}\phi''_{s+t}(x).$$

Finally, in the case when $(s, t) = (2, -1)$ or $(s, t) = (3/2, -1/2)$, the function $\phi_{s+t} = \phi_1$ is the Gauss density, so that

$$\log 2 \cdot \phi_{(2,-1)}(x, 0) = \frac{1}{3}\left(\frac{1}{(1+x)} + \frac{1}{(1+x)^2} + \frac{1}{(1+x)^3}\right), \tag{37}$$

$$\log 2 \cdot \phi_{(3/2,-1/2)}(x, 0) = \frac{1}{2}\left(\frac{1}{(1+x)} + \frac{1}{(1+x)^2}\right). \tag{38}$$

3.6 Step 2, continued. Behaviour of the series $T_i(s)$ at $s = 1$.

We will prove the following:

Proposition 8 *There exists a neighborhood of $s = 1$ [which depends on the admissible function F] on which each series $T_i(s)$ has a unique pôle, simple and located at $s = 1$, with a residue of the form $(6/\pi^2)A_i$. The constant A_0 equals 1 and $A := A_1 + A_2 + A_3 + A_4$ is equal to*

$$A = \frac{2}{3} + \frac{1}{4\log 2}.$$

Proof: With the spectral decomposition of operators of $\mathcal{G}_s$, each operator $\mathbf{M}_i(s)$ decomposes itself into a dominant term and three remainder terms.

We study first the dominant term, where each operator $\mathbb{G}_s, \mathbb{L}_s$ is replaced by its dominant term. The dominant part of each $\mathbf{M}_i(s)$ is of the form

$$\left(\sum_p \lambda(s)^p\right) \cdot \mathbf{B}_s^{[i]} = \mathbf{B}_s^{[i]} \cdot \frac{1}{1-\lambda(s)}$$

for some operator $\mathbf{B}_s^{[i]}$ which involves the dominant projectors $\mathbb{P}_s$ and the bounded operator $\mathbf{A}_s$ of Proposition 3, and it thus has a pôle at $s=1$. Then, with Proposition 3, each series $T_i(s)$ has a pôle at $s=1$, with a residue equal to[(ii)]

$$\frac{-1}{\lambda'(1)}\mathbf{B}_1^{[i]}[\mathbb{F}_1^{[i]}](\underline{0}) = \frac{-1}{\lambda'(1)} \cdot \frac{1}{\log 2} \cdot A_i = \frac{6}{\pi^2} \cdot A_i,$$

where $\mathbb{F}_s$ is the dominant eigenfunction relative to the operator $\mathbb{L}_s$ of Proposition 3. With the remarks of Section 3.5, and expression of $\mathbf{Q}_1$ provided in (36), each A_i admits a precise expression:

$$A_0 = 1, \qquad A_1 = 2\int_0^1 \phi_{(3/2,-1/2)}(x,0)\ \mathrm{d}x, \qquad A_2 = -\int_0^1 \phi_{(2,-1)}(x,0)\ \mathrm{d}x$$

$$A_3 = \int_0^1 \mathbf{H}_{(3/2,\cdot)}[\phi_{(3/2,-1/2)}](x,0)\ \mathrm{d}x, \qquad A_4 = -\int_0^1 \mathbf{H}_{(3/2,\cdot)}[\phi_{(2,-1)}](x,0)\ \mathrm{d}x.$$

On the other hand, each $\mathbf{M}_i(s)$ gives rise to three remainder terms, each of them being obtained when at least one of the two operators $\mathbb{G}_s, \mathbb{L}_s$ is replaced by its remainder term $\mathbb{R}_s$ [see Proposition 4, *(iii)*]. Each remainder term can be written as a series of operators, whose norm is upper bounded respectively (up to absolute multiplicative constants) by

$$\sum_p |\lambda(s)|^{p-F(p)} \cdot \nu(s)^{F(p)}, \qquad \sum_p |\lambda(s)|^{F(p)} \cdot \nu(s)^{p-F(p)} \qquad \sum_p \nu(s)^p.$$

when s is near 1. (Here, $\nu(s)$ is any constant strictly less than 1 and strictly larger than the subdominant spectral radius of operators $\mathbb{G}_s$ and $\mathbb{L}_s$ which appear in Proposition 3). For any constant $d>0$, there exists a neighborhood $\mathcal{V}_d$ of $s=1$ on which the inequalities $|\lambda(s)| \leq \nu(s)^{-d}$, $\nu(s)<1$ hold. This entails that the previous general terms are less than $\nu(s)^{c(p)}$ with $c(p) := \min(-dp+(d+1)F(p), p-(d+1)F(p))$. Since F is admissible with parameters a,b [with $0<a<b<1$], choosing d as

$$d_0 := \frac{1}{2}\min\left(\frac{1-b}{b}, \frac{a}{1-a}\right)$$

ensures the existence of a constant $c>0$ for which $c(p) \geq c \cdot p$. Then, on the neighborhood $\mathcal{V}_{d_0}$, the general term of each series is upper bounded by a term of the form $\nu(s)^{cp}$, when s is in a

(ii) The relation $\lambda'(1) = -\pi^2/(6\log 2)$ can be deduced from the equality between the two expressions of $T_0(s)$ given in the proof of Proposition 3.

complex neighbourhood of $s = 1$. Then, each of the three remainder terms defines an operator which is analytic on $\mathcal{V}_{d_0}$.

Computation of constant $A_1 + A_2$. With the expression of $\phi_{(2,-1)}$ and $\phi_{(3/2,-1/2)}$ provided in (37,38), the first constant $A_1 + A_2$ satisfies

$$A_1 + A_2 = \frac{1}{\log 2} \int_1^2 \frac{1}{3} \left(\frac{2}{y} + \frac{2}{y^2} - \frac{1}{y^3} \right) \mathrm{d}y = \frac{2}{3} + \frac{5}{24 \log 2}.$$

Computation of constant $A_3 + A_4$. With the change of variables $w = 1/(m + x)$, one obtains

$$\begin{aligned} \int_0^1 \mathbf{H}_{(s,\cdot)}[F](x,y)\ \mathrm{d}x &= \int_0^1 \sum_{m \geq 1} \frac{1}{(m+x)^{2s}} F\left(\frac{1}{m+x}, y \right)\ \mathrm{d}x \\ &= \sum_{m \geq 1} \int_{1/(m+1)}^{1/m} w^{2s-2} \cdot F(w,y)\ \mathrm{d}w = \int_0^1 w^{2s-2} \cdot F(w,y)\ \mathrm{d}w. \end{aligned}$$

Then, with Relations (37,38), the constant $A_3 + A_4$ equals

$$\begin{aligned} A_3 + A_3 &= \int_0^1 x \left(\phi_{(3/2,-1/2)} - \phi_{(2,-1)} \right)(x,0)\, \mathrm{d}x \\ &= \frac{1}{\log 2} \int_1^2 (y-1)\left(\frac{1}{6y} + \frac{1}{6y^2} - \frac{1}{3y^3} \right) \mathrm{d}y = \frac{1}{24 \log 2} \end{aligned}$$

This finally leads to the equality $A = A_1 + A_2 + A_3 + A_4 = \dfrac{2}{3} + \dfrac{1}{4 \log 2}$. □

3.7 Step 2, concluded. Bounds à la Dolgopyat for operators of $\mathcal{G}_s$.

Here, we now focus on the behaviour of operators $\mathbb{G}_s$ on vertical strips near $s = 1$.

Proposition 9 *Consider any operator* $\mathbb{G}_s$ *of* $\mathcal{G}_s$. *For any* $\xi > 0$, *there exist* $\beta > 0$, $M > 0$, $\gamma < 1$, *for which, when* s *belongs to the vertical strip* $|\Re s - 1| \leq \beta$, *with* $\tau := \Im s$ *satisfying* $|\tau| > \tau_0 > 0$, *the* n*-th iterate of the operator* $\mathbb{G}_s$ *satisfies:*

$$||\mathbb{G}_s^n||_{1,\tau} \leq M \cdot \gamma^n \cdot |\tau|^\xi, \qquad \text{for } n \geq 1.$$

(Here, the norm $||\cdot||_{1,\tau}$ *is defined as* $||F||_{1,\tau} := ||F||_0 + (1/|\tau|)||F||_1$.*)*

Proof: A detailed proof of this result will appear in a forthcoming paper [5]. Here, we shall provide only a sketch of the proof. From works of Dolgopyat [7], improved by Baladi and Vallée [4], we already know that this property holds for the plain operator $\mathbf{H}_s$. We now prove that this property extends to other operators of $\mathcal{G}_s$, which act on functions of several variables.

In the case of the operator $\mathbf{H}_{(s,\cdot)}$, the existence of a constant K for which the relation $||\mathbf{H}_{(s,\cdot)}^n||_{1,\tau} \leq K||\mathbf{H}_s^n||_{1,\tau}$ holds for any $n \geq 1$ is sufficient to entail the property.

In the case of operators of $\mathcal{G}_s^{(1)}$, the central remark is the following: we recall that, in the case of one variable, the key part of Dolgopyat's method (see [4]) involves the integral

$$\mathbf{Q}_1[|\mathbf{H}_s^n[f]|^2] := \int_0^1 |\mathbf{H}_s^n[f](w)|^2 \, \mathrm{d}w,$$

which is evaluated in Lemmata 4 and 5 of the cited paper. In the case of a general operator $\mathbb{G}_s$ of $\mathcal{G}_s^{(1)}$, this integral is a priori replaced by the quantity $\mathbb{Q}_1[|\mathbb{G}_s^n[F]|^2]$ which involves the value at $s = 1$ of the dominant eigenvector $\mathbb{Q}_s$ of the dual operator $\mathbb{G}_s^\star$. We know, with Section 3.5, that the dominant eigenvector $\mathbb{Q}_s$ at $s = 1$ is defined by the integral of a diagonal mapping, so that the sequence of equalities

$$\mathbb{Q}_1[|\mathbb{G}_s^n[F]|^2] = \mathbf{Q}_1[\mathrm{diag}\,(|\mathbb{G}_s^n[F]|^2)] = \mathbf{Q}_1[|\mathrm{diag}\,(\mathbb{G}_s^n[F])|^2]$$

$$= \mathbf{Q}_1[|\mathbf{H}_s^n[\mathrm{diag}\,F]|^2] = \int_0^1 |\mathbf{H}_s^n[\mathrm{diag}\,F](w)|^2 \, \mathrm{d}w$$

holds and entails that the proof of Dolgopyat-Baladi-Vallée for operator $\mathbf{H}_s$ easily extends to the case of a general operator $\mathbb{G}_s$ of the set $\mathcal{G}_s^{(1)}$. □

Now, with the general form of the operators $\mathbf{M}_i(s)$, these bounds à la Dolgopyat entail that

$$||\mathbf{M}_i(s)||_{1,\tau} \leq K_1 \cdot \frac{1}{1-\gamma} \cdot |\tau|^{2\xi}. \tag{39}$$

for some constant K_1, when s satisfies $|\Re s - 1| \leq \beta$, with $|\tau| > \tau_0 > 0$. This entails a bound on the same type for the Dirichlet series $T_i(s)$.

Finally, with Propositions 8 and 9, returning to Dirichlet series proves:

Proposition 10 *There exist $\xi < 1/2$, $\alpha > 0$, $K > 0$ for which each Dirichlet series $T_i(s)$ satisfies the following:*

(i) It has a unique pôle inside the vertical strip $|\Re s - 1| \leq 4\alpha$, located at $s = 1$, simple.

(ii) On the left line $\Re s = 1 - 4\alpha$, one has $|T_i(s)| \leq K \max(1, |\tau|^{2\xi})$.

3.8 Step 3. Extraction of coefficients.

Then, all the conditions are fulfilled for applying with success the Perron formula. As in [4], the Perron formula first gives us estimates on the sums $\Psi(U), \Psi_0(U)$, defined in (15)

$$\Psi(U) = \frac{6A}{\pi^2}\left(\frac{U^3}{3}\right)\left(1 + O(U^{-4\alpha})\right), \qquad \Psi_0(U) = \frac{6}{\pi^2}\left(\frac{U^3}{3}\right)\left(1 + O(U^{-4\alpha})\right).$$

These estimates can be transfered first on the so–called smoothed versions $\overline{\Phi}(p), \overline{\Phi}_0(p)$ of the partial sums

$$\Phi(p) := \sum_{n \leq p} a_n, \qquad \Phi_0(p) := \sum_{n \leq p} b_n,$$

with Lemma 11 of [4][(iii)]. We then obtain

$$\overline{\Phi}(p) = \frac{6A}{\pi^2}\left(\frac{p^2}{2}\right)\big(1+O(p^{-2\alpha})\big) \qquad \overline{\Phi}_0(p) = \frac{6}{\pi^2}\left(\frac{p^2}{2}\right)\big(1+O(p^{-2\alpha})\big).$$

We then obtain an estimate for the so–called smoothed version of the expectation

$$\overline{\mathbb{E}}_N[S_{<F>}] = A\cdot\big(1+O(N^{-2\alpha})\big),$$

By using the arguments of Lemma 14 of [4], we obtain the final estimate for the unsmoothed version of the expectation,

$$\mathbb{E}_N[S_{<F>}] = A\cdot\big(1+O(N^{-\alpha})\big),$$

which proves our Theorem 1.

4 Conclusion

We then provide a precise answer to the question of Arnold, when the random pairs (a,n) belong to the set Ω_N defined in (4). We show that the arithmetic progressions do not behave at all as "random" modular sequences, since the constant A is very close to 1. Moreover, we prove that the probabilistic behaviour of Arnold's sum is highly independent on the precise choice of the index k of the continuant q_k, since this choice may only influence the remainder term.

However, there are two important remarks to be done:

(i) First, our probabilistic study is performed on the set Ω_N which contains all the coprime pairs (a,n) that satisfy $a \le n \le N$. With our methods, we do not succeed to obtain this probabilistic behaviour on each subset ω_n formed with pairs (a,n) with a fixed n. Such a result is certainly quite difficult to obtain.

(ii) The choice of $T = q_k$ proposed by Arnold is certainly one of the worst possible choices, since, in this case, there are only two possible distances. There exist other choices of parameter T for which there are only two possible distances, when T is equal to $q_{k-1} + \alpha q_k$, for an integer α that satisfies $0 < \alpha \le m_{k+1}$. And, for a value of T, of the form $q_{k-1} + \alpha q_k + \beta$, with $0 < \alpha \le m_{k+1}$ and $0 < \beta < q_{k-1}$, there are exactly three possible distances. In a forthcoming paper, we will make precise the behaviour of modular arithmetic progressions for a general choice of the parameter T, with respect to parameters α, β.

References

[1] J.-P. Allouche, J. Shallit, *Automatic sequences. Theory, Applications, Generalizations*, Cambridge, 2005.

[2] V. I. Arnold, *Arnold's problems*, Springer Phasis, 2004.

[3] V. I. Arnold, *Topology and statistics of formulae of arithmetics*, Russian Math. Surveys **58** (2003), 637–664.

(iii) The results provided in Lemmas 11 and 14 of [4] are correct, even if the smoothed probabilistic model used is not the convenient one. This part of the paper [4] is corrected in [5]

[4] V. Baladi, B. Vallée, *Euclidean algorithms are Gaussian*, J. Number Theory **110** (2005), 331–386.

[5] E. Cesaratto, *Remarks and extensions on the paper "Euclidean Algorithms are Gaussian" by Baladi and Vallée*, in preparation.

[6] M. Deléglise, *Recouvrement optimal du cercle par les multiples d'un intervalle*, Acta Arith. **59** (1991), 21–35.

[7] D. Dolgopyat, *On decay of correlations in Anosov flows*, Ann. of Math. (2) **147** (1998), 357–390.

[8] G.H. Hardy, E.M. Wright, *An introduction to the Theory of Numbers*, 5th edition, Oxford Clarendon Press, 1979.

[9] D. E. Knuth, *The art of Computer Programming, Volume 2*, Third Edition, Addison Wesley (1998)

[10] A. Plagne, *À propos de la fonction X d'Erdös et Graham*, Ann. Inst. Fourier (Grenoble) **54** (2004), 1717–1767.

[11] D. Ruelle, *Thermodynamic formalism*, Addison Wesley, 1978.

[12] V. T. Sós, *On the distribution mod* 1 *of the sequence* $n\alpha$, Ann. Univ. Sci. Budapest Eötvös Sect. Math. **1** (1958), 127–134.

[13] J. Stern, *Secret linear congruential generator are not cryptographically secure*, Proc of the IEEE Symposium on Foundations of Computer Science (1987), 421-426.

[14] J. Surányi, *Über die Anordnung der Vielfachen einer reellen Zahl mod* 1, Ann. Univ. Sci. Budapest Eötvös Sect. Math. **1** (1958), 107–111.

[15] S. Świerczkowski, *On successive settings of an arc on the circumference of a circle*, Fund. Math. **46** (1959), 187–189.

[16] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, Cours Spécialisés 1, SMF, 1995.

[17] B. Vallée, *Euclidean dynamics*, Discrete Contin. Dyn. Syst. **15** (2006), 281–352.

[18] B. Vallée, *Opérateurs de Ruelle-Mayer généralisés et analyse en moyenne des algorithmes de Gauss et d'Euclide*, Acta Arith. **81** (1997), 101–144.